Militärische Gewalt bei Cyberattacken

Heikle Ansichten einer der Nato nahestehenden Expertengruppe zum Recht auf Selbstverteidigung

Von der Öffentlichkeit kaum beachtet, hat eine Expertengruppe einen «Leitfaden» zum Verhältnis von Völkerrecht und Cyberangriffen publiziert. Dieses «Tallinn-Manual» weicht die Schranken zulässiger Gewaltanwendung in problematischer Weise auf.

Oliver Diggelmann

Cyberangriffe können Zehntausende von Computern und ganze Bargeldbezugssysteme gleichzeitig lahmlegen. Im März traf eine Attacke mehrere Rundfunkanbieter und Banken in Südkorea, wobei der Angreifer nicht genau festgestellt werden konnte. Ziele sind zunehmend nicht nur einzelne Computer, sondern ganze Rechen- und Steuerungszentren. Im Januar zielte eine Angriffswelle auf die Zentren der 20 grössten Banken der USA. Dazu bekannte sich eine Gruppierung namens Izz ad-Din al-Kassam Cyber Fighters; die USA schrieben den Angriff Iran zu. Möglicherweise war die aufwendige Operation eine Vergeltungsaktion für durch den Computerwurm Stuxnet 2010 verursachte Schäden. Es wird vermutet, dass Israel oder die USA Urheber oder Auftraggeber des Angriffs waren, der damals Teile der der iranischen Uran-Anreicherungs lahmlegte.

Verheerende Folgen denkbar

Zu Todesopfern haben Cyberattacken bisher nicht geführt. Die wirtschaftlichen Schäden aber sind enorm. Cyberattacken und Phishing zusammen sollen jährlich weltweit Schäden in der Grössenordnung von 110 Milliarden Dollar verursachen. Dass sie nur wirtschaftlicher Natur sind, braucht nicht so zu bleiben. Szenarien mit kriegsähnlichen Wirkungen sind denkbar geworden. Sollte es Angreifern gelingen, die Kontrolle über Teile eines Stromversorgungsnetzes zu gewinnen und dieses auszuschalten, so stünden Menschenleben auf dem Spiel. In kalten Regionen könnten Menschen erfrieren, in Spitälern viele sterben. Manipulationen bei der Steuerung des Zugverkehrs könnten zu Kollisionen von Zügen führen.

Wie verhält sich das Völkerrecht zu dieser neuartigen Form von Angriffen? Über diese Frage wird unter dem Stichwort des Cyberwar diskutiert. Wichtig ist zunächst: Es handelt sich eben gerade nicht um einen Krieg, bei dem sich Armeen gegenüberstehen. Gemeinsam sind allenfalls kriegsähnliche Elemente. Das wirft völkerrechtlich schwierige Fragen auf. Eine überragt alle anderen an Bedeutung: Wann kann sich ein Staat auf sein Recht auf Selbstverteidigung berufen und sich gewaltsam gegen Cyberattacken zur Wehr setzen?

Gemäss der Uno-Charta und Gewohnheitsrecht ist das Kriterium des «bewaffneten Angriffs» entscheidend. Während eines solchen ist militärische Verteidigung ohne Autorisierung durch den Uno-Sicherheitsrat zulässig. Doch kann man bei Cyberattacken von «bewaffneten Angriffen» sprechen? Mit diesem und anderen Problemen hat sich eine international zusammengesetzte Gruppe von Völkerrechtlern und Militärpersonen – überwiegend aus den USA und aus Europa – während mehrerer Jahre befasst. Ins Leben gerufen wurde sie von einem von den Nato-Mitgliedstaaten finanzierten Think-Tank. Dieser hat seinen Sitz in Tallinn in Estland, das 2007 Ziel eines massiven russischen Cyberangriffs geworden war.

Territoriales Element

Die Expertengruppe hat das Ergebnis ihrer Arbeit vor kurzem in Form eines «Leitfadens» publiziert, des «Tallinn-Manual zur Anwendung des Völkerrechts auf die Cyberkriegsführung». Es enthält eine Auslegeordnung der sich beim Verhältnis zwischen Völkerrecht und Cyberwar stellenden Probleme, ist inhaltlich aber teilweise heikel, ja brisant. Nicht nur deshalb, weil es seinen Weg zu Entscheidungsträgern mächtiger Nato-Staaten finden dürfte, sondern vor allem, weil die Ansichten zum Selbstverteidigungsrecht die Grenzen völkerrechtlich zulässiger Gewaltanwendung aufweichen.

Laut dem Manual liegt bei Cyberangriffen zunächst dann ein bewaffneter Angriff vor, wenn die Wirkungen jenen herkömmlicher bewaffneter Angriffe gleichkommen. Man denke etwa an Manipulationen an Zug- oder Flugsteuerungssystemen, die zu Zusammenstössen führen und den Verkehr lahmlegen, oder an Eingriffe in die Regulierung eines Staudammes, die die Überschwemmung eines Tals zur Folge hat. Solche Wirkungen können auch die Folge eines herkömmlichen Angriffs sein. Die Position der Expertengruppe ist in diesem Punkt plausibel. Das Manual lässt es damit aber nicht bewenden. Es wirft auch die Frage auf, ob blosse finanzielle Schädigungen eines Staates durch Cyberangriffe zur gewaltsamen Selbstverteidigung berechtigen, wenn sie katastrophale Ausmasse annehmen. Ein Teil der Experten bejaht dies. Vor Augen haben sie das Szenario eines Börsenabsturzes.

Die Bejahung des Rechts auf Selbstverteidigung in einem solchen Fall würde das Recht gegenüber dem herkömmlichen Verständnis grundlegend verändern. Auf das Erfordernis eines physisch-territorialen Elements – das beim herkömmlichen bewaffneten Angriff stets vorliegen muss – würde nun ganz verzichtet. Traditionell besteht es etwa darin, dass ein Teil des Staatsgebiets von einem anderen Staat besetzt wird, auch wenn kein Widerstand geleistet wird. Oder es besteht darin, dass die auf dem Territorium lebende Bevölkerung oder die Infrastruktur durch den Einsatz von Waffen wie Raketen physisch geschädigt wird. Dieses physisch-territoriale Element ist herkömmlich das Objekt der Verteidigungshandlung, zu der das Selbstverteidigungsrecht autorisiert.

Würde ein finanzieller Schaden genügen, so könnte sich die Selbstverteidigung nicht mehr gegen konkrete physische Vorgänge richten, sondern nur noch gegen den anderen Staat generell. Es gäbe keine konkreten physischen Vorgänge, die mittels eigener Gewalt beendet oder abgewehrt werden könnten. Das würde den Charakter der Selbstverteidigung verändern: Die Idee der Beendigung würde in den Hintergrund gedrängt, der Vergeltungs- und Abschreckungsgedanke würde leitend.

Prinzip des Gewaltverbots

Damit entfernt man sich weit von den Grundideen des Rechts auf Gewaltanwendung – wohl zu weit. Die Uno-Charta und das Gewohnheitsrecht verbieten Gewalt zwischen Staaten zunächst einmal kategorisch. Sie durchbrechen diesen Grundsatz nur punktuell, mit klar benennbaren Prinzipien. Über allen steht die Idee, dass Gewaltanwendung kein zulässiges Sanktions-

mittel für Völkerrechtsverletzungen ist – ausser der Sicherheitsrat autorisiere sie. Das Recht auf Selbstverteidigung basiert auf dem Gedanken, dass eine Möglichkeit zur gewaltsamen Beendigung gewaltsamer Verletzungen des Territoriums bestehen soll, des Territoriums als der existenziellen Grundlage des Staates. In der zeitlichen Einschränkung sodann, dass Selbstverteidigung nur während des Angriffs geübt werden darf, kommt der Charakter des Selbstverteidigungsrechts als eines Beendigungs- und nicht eines Vergeltungsrechts zum Ausdruck. Beide Erfordernisse zusammen schränken den Bruch des Gewaltverbots und das Recht zur eigenmächtigen Gewalt ein.

Genau hier öffnet das Manual aber heikle Schleusen. Wenn bei einem Börsencrash ein Selbstverteidigungsrecht bestehen soll, dann wird es in der Substanz zu einem Recht auf gewaltsame Vergeltung schwerwiegender Schädigungen der Wirtschaft. Ein solches Ergebnis mag in der Abschreckungslogik von Cyberwar-Szenarien erstrebenswert erscheinen, in denen Konsequenz und Glaubwürdigkeit die zentralen Werte sind. Mit den Grundideen des Völkerrechts ist es aber nicht kompatibel. Autorisieren kann die Gewaltanwendung bei Cyberattacken mit finanziellen Folgen nur der Sicherheitsrat, wenn er eine Friedensbedrohung feststellt.

Die Schleusen nicht öffnen

Dazu kommt, dass das Kriterium katastrophaler finanzieller Schäden missbrauchsanfällig ist. Was gilt etwa bei einem nur kleinen Börsencrash oder bei einem Angriff auf einen volkswirtschaftlich relevanten Konzern? Kaum lösbare Probleme bereitet auch die sogenannte antizipatorische Selbstverteidigung. Sie wird als zulässig betrachtet, wenn ein Angriff unmittelbar bevorsteht und nicht anders als durch Gewalt abwendbar ist. Wann aber soll dies bei Cyberattacken genau der Fall sein, anhand welcher Kriterien soll man dies beurteilen? Auch hier würde missbräuchlicher Berufung auf das Selbstverteidigungsrecht Tür und Tor geöffnet. Betonung verdient weiter, dass der Angreifer bei vielen Cyberattacken nicht zweifelsfrei ermittelt werden kann. Ein Gegenschlag, ob im Cyberspace oder real geführt, würde zum Schuss in den Nebel.

Man kann sich fragen: Soll die Formulierung von Antworten auf derart wichtige Fragen auf Dauer Gremien überlassen werden, die eine überdurchschnittliche Nähe zum Militär aufweisen? Beim «Tallinn-Manual» besteht eine solche Nähe – und auch der Eindruck, dass sie sich auch auf den Inhalt ausgewirkt hat. Ich meine daher nein.

Oliver Diggelmann ist Professor für Völker- und Staatsrecht an der Universität Zürich.